Hindawi
Wireless Communications and Mobile Computing
Volume 2020, Article ID 8815461, 10 pages
https://doi.org/10.1155/2020/8815461

Research Article

Remote Identity Verification Using Gait Analysis and Face Recognition

Wen Si,[1,2] Jing Zhang ,[1] Yu-Dong Li,[1] Wei Tan,[3] Yi-Fan Shao,[4] and Ge-Lan Yang[5]

[1] *Faculty of Business Information, Shanghai Business School, Shanghai 200235, China*
[2] *Department of Rehabilitation, Huashan Hospital, Fudan University, Shanghai 200433, China*
[3] *School of Computer Science and Technology, Dongguan University of Technology, Dongguan 523830, China*
[4] *ECE in University of Michigan-Shanghai Jiao Tong University Joint Institute at Shanghai Jiao Tong University, Shanghai 200240, China*
[5] *Department of Information Science and Engineering, Hunan City University, Yiyang 413000, China*

Correspondence should be addressed to Jing Zhang; zhangjing25@163.com

Received 2 September 2020; Revised 4 October 2020; Accepted 31 October 2020; Published 23 November 2020

Academic Editor: Hongju Cheng

Biometric identification has verified its effectiveness in personal identity verification because of the uniqueness and noninvasion. In this research, we tend to apply the detection of biometric information to a remote sensing system for the purpose of security area monitoring. Our system is established by collecting signals from the coming individuals via the remote measurement in the specific condition where both kinds of data are detected to determine the identity. Specifically, the measuring of gait signals and facial images is integrated to provide a way of improving the detection accuracy and the robustness. In addition, the fuzzy association rule (FAR) is employed for data analysis in line with the outcomes of different methods. As such, the signals are integrated and transmitted for further processing and remote identification. Experiments are conducted to demonstrate the capability of the proposed system. With the training data increases, a high detection accuracy of 95.2% is obtained, which makes it a promising basis for the realization of remote identity verification.

1. Introduction

Automatic verification of an individual's identity has already become a practical and creative tool in a wide range of applications, especially in the access to some high-restricted environment [1]. In view of certification, the identity verification indicates that an identity is confirmed to be real, together with the individual claiming the identity entitled to him [2]. In accordance with the *Good Practice Guide* (GPG), the verification of personal identity generally starts with collecting the information to pick a person from the population of interest [3]. Rather than using magnetic cards or pin numbers, current studies pay more attention to more convenient, easy, and remote sensing methods in practical use [4, 5]. Specifically, for places of high security and secrecy demands, such as government agencies, scientific laboratories, archives, or the national border, the employment of an optimal remote identity verification method with high accuracy is most pronounced [6]. For these reasons, research is still ongoing to develop identity verification devices and strategies.

Notably, biometrics has already been used for decades as one of the strongest methods to identify and authenticate individual identity [7]. Explicitly, biometrics can be regarded as the technical term for human body measurements and calculations. It refers to the metrics related to all human characteristics. Biometric technology, which is widely spread due to its high accuracy and user friendliness, is currently employed for recognizing individuals via measurable physiological or behavioural properties [8]. To the best of our knowledge, the physiological properties include fingerprint [9], iris [10], and face [11], while the behavioural properties include tread [12], signature [13], and voice [14]. To this end, by transferring the biometric properties into electric signals, we are thus able to get insight into the system of using biometrics to describe individuals [15].

In spite of the restrictions to our daily life circumstances, the remote access to biometric parameters has greatly progressed with advances in signal collecting and processing devices. It is obvious that the biometric measurement can be attached to real personal activities within a long distance, whose physiological or behavioural traits can be recorded. Nevertheless, one major problem involved with biometrics detection is that the physical appearance of a person may vary with time and environment [16], whereas a 100% accurate measurement rate is impossible to get by merely sensing one single kind of biometric parameter. For this reason, a possible resolution for addressing this issue is to integrate several biometrics into one system. However, since so many biometric parameters are involved in the identity verification, we employ the fuzzy association principle (FAR) for determination in this paper, which is widely used in data mining and decision support application. As such, the sensing signals can be applied for remote identification. The measurement devices, which are suitable for daily ambulatory signal collecting, are designed to meet this requirement for personal identity verification in security and secrecy areas [17].

In this research, we aim to establish a remote identity verification strategy specifically for high-security-monitoring area based on daily life activities. Concerning the analysis of biometric properties, we take the facial images and the gait data measurement during individual walking towards the target place due to its high precision and easy implementation. To this end, the task is addressed by integrating a set of data analysis algorithms for real-time individual biometrics detection and description.

The remaining part of this paper is organized as follows. Related work about gait analysis, face recognition, and the FAR is reviewed in Section 2. Section 3 illustrates the devising of remote signal acquisition system as well as its working procedure. In Section 4, the measurement mechanism and the data processing methodologies for feature extraction and individual recognition are presented. The working performance of the proposed approach is verified by experiments in Section 5. Concluding remarks are given in Section 6.

2. Related Work

2.1. Gait Analysis. Walking is characterized by gait [18]. Gait analysis is initially proposed for precisely quantifying the functional integration while walking by using various strategies [19, 20]. For instance, as one of the commercial walkway devices, the GAITRite system has identified its distinguishing exploration in providing a reliable approach for detecting both averaged and individual gait parameters of the elderly [21, 22].

Gait analysis is typically carried out relying on either of the two ways, including visual observations and motion laboratory devices [23]. The former is aimed at observing the subject's locomotion via cameras during walking while the latter is equipped with sensors for analyzing the gait variation. Nonetheless, the outcomes of the observation approach are qualitative and unreliable. In most cases, the motion measurement system provides precise results based on highly accurate sensing setups such as electromyography systems and joint accelerometers [24, 25]. From a biomechanical point of view, ground reaction forces can be explained by Newton's third law—for every action, there is an equal and opposite reaction of the human foot pressure, which is a way of describing human gait [26]. State-of-the-art studies find that the ground reaction addresses the evaluation of muscle forces, joint torques, and stiffness of damping associated with leg-surface contact [27]. Specifically, the ground reaction force (GRF) measurement is noninvasive and easy to implement. In this way, GRF is one of the distinctive, measurable characteristics used to label and describe individuals.

2.2. Face Recognition. Face recognition indicates the detection of face from cluttered background in line with the recognition using a database of facial characteristics [28]. Typically, the face image of a person is obtained from a video source. The development of face recognition technology largely depends on the flourish of machine learning and deep learning algorithms [29]. There are multiple methods in which face recognition systems work, but in general, they work by comparing selected facial features to determine whether the two face images belong to the same person or not [30]. To this end, face recognition can be primarily carried out via the following steps: (i) face detection: in the first place, we categorize the variation of colors from the input image and find the location and size of the faces in this image [31]; (ii) feature extraction: feature extraction is a most critical procedure which takes the biometric features, such as color of the eyes and width of the nose to construct a feature representation of the target face [32]; (iii) facial recognition: the feature representation of a face is commonly in the form of matrix, which is taken as the input of the facial recognition system [33]; and (iv) individual tagging: the person identity is determined by searching the current database. In this way, a name is tagged to the person whose image has already been captured [34].

To keep the method user-friendly, the four steps are taken in real time [35]. In this way, with a camera employed for image collecting, the face recognition process can be carried out for person identity verification.

2.3. Fuzzy Association Rules (FAR). Theoretically, fuzzy association rules are utilized to capture the correlations between low-level features and high-level essence of the target [36]. We now give a brief description of this principle.

$$X = \{x_1, x_2, \cdots, x_n\}. \tag{1}$$

Let it be the initial database, together with all the characteristics in$X$.

$$T = \{t_1, t_2, \cdots, t_m\}. \tag{2}$$

Specifically, we carry out a fuzzy set associated with each characteristic [37]. For the characteristic t_i, the fuzzy set indicating the internal property of t_i is given as follows:

$$F_{t_i} = \left\{ f_{t_i}^1, f_{t_i}^2, \cdots, f_{t_i}^k \right\}. \tag{3}$$

For the purpose of biometric parameter identification, we shall thus define Gait $= \{g_1, g_2, \cdots, g_n\}$ as the gait feature and Image $= \{i_1, i_2, \cdots, i_m\}$ as the facial image feature. Supposing that $F_{\text{gait}} = \{f_{g1}, f_{g2}, \cdots, f_{gn}\}$ and $F_{\text{image}} = \{f_{i1}, f_{i2}, \cdots, f_{\text{in}}\}$ refer to the corresponding properties or gait and face feature, respectively. As for each pair of (g_j, f_{gj}) or (i_j, f_{ij}), we call it an item. Similarly, each pair of (Gait, F_{gait}) or (Image, F_{image}) is an itemset.

Hence, in order to find the internal correlation, the Gait $\rightarrow F_{\text{gait}}$ can be derived from Image $\rightarrow F_{\text{image}}$ based on FAR. As such, we can get votes which are greater than the specific threshold of the dataset. In other words, the probability that Image occurs given that Gait has occurred is defined as the confidence of the rule [38, 39]. In this way, the significance factor of (Gait, F_{gait}) is presented as follows:

$$\text{Significance} = \frac{\text{Sum of voting for } \left(\text{Gait}, F_{\text{gait}}\right)}{\text{Number of records in identity } P}, \tag{4}$$

where P is the dataset of individual identity features whose fuzzy set is F_p. Mathematically, $P = \text{Gait} + \text{Image}$ and $F_p = F_{\text{gait}} + F_{\text{image}}$. On the other hand, the certainty factor for supporting the rule is given as follows:

$$P\left\{ \left(\text{Gait}, F_{\text{gait}}\right), \left(\text{Image}, F_{\text{image}}\right) \right\} \frac{\sum_{p_i \in P} \prod_{F_{pi} \in F_p} \left\{ \alpha\left(in_i \middle| f_p \middle| \right) \right\}}{\sum_{p_i \in P} \prod_{g_j \in \text{Gait}} \left\{ \alpha\left(in_i \middle| g_j \middle| \right) \right\}}, \tag{5}$$

where function α is to compute the voting in comparison the threshold value. In addition, in_i indicates the i^{th} person within the permitted individual dataset.

3. System Architecture

Considering the biometric parameter measurement, a system is established aiming at verifying the person identity by using the biometric characteristics for security monitoring. There are two parts in the system, which are gait analysis part and face recognition part. The outcomes of each part are integrated to determine the identity of the coming person (Figure 1). The deployment of both parts is illustrated as follows.

3.1. GRF Testing Setup. In this paper, a strain gauge force platform with the size of 400 mm × 2000 mm is employed to collect the GRFs of both feet on the laboratory walkway while walking. Apparently, the more sensing elements are placed, the higher precision of GRF can be measured [40]. Within this force plate, 256 vertical electrode sheets and 128 horizontal electrode sheets are employed for sensing. The force platform is calibrated by the calibration matrix provided by the manufacturer before putting into practical application. The detection of GRF can easily be implemented, as shown in Figure 2. As long as a force plate is set to establish a walking foot fall, the data will be automatically recorded when someone walks on it at free speed. The GRF signals are transmitted into voltage values with respect to the force applied on the sensor surface. Based on the input signals, the sensing data is sent to a signal acquisition module (NI FD-11637) with a highest sampling rate as 100 kS/s [41]. The force signals are sampled at a frequency of 500 Hz in this system. The acquisition device has the function of signal amplifying as well as a 24-bit analog-digital conversion for data transforming. What is more, a host computer is connected directly to the signal acquisition hardware via USB. As such, the GRF outcomes can subsequently be stored and provided for further analysis. Thereby, this data collection device, on the basic of GRF sensing, can be attached to the individual verification system whenever required.

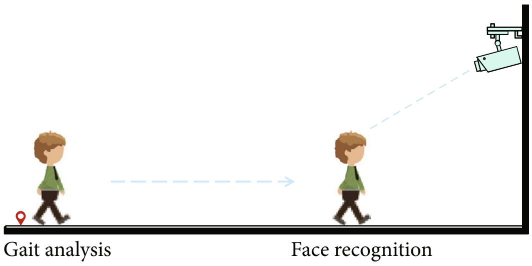

FIGURE 1: System deployment.

There are three components measured by using the force plate, which are as follows:

(i) F_z: vertical component on Z axis

(ii) F_y: horizontal component on Y axis (anterior-posterior)

(iii) F_x: horizontal component on X axis (medial-lateral)

We thus have GRF $= \{F_x, F_y, F_z\}$. The total GRF can therefore be represented by a vector that is the sum of the vertical load as well as the shear force in two orthogonal directions. The components of GRF are illustrated in Figure 3.

3.2. Face Recognition Setup. For the purpose of image detection, a visual sensing module integrates cameras to collect time series scenarios and characterize and identify intrusion targets [42, 43]. In this paper, since the individual's digital face image acquired from a sensor is compared with the face images in the database, a Panasonic WV-CW590CH detection camera with a 650 color dpi is deployed in front of the security door. This instrument is able to detect objects within a range of 10 meters and is hard wired to a DC-regulated power supply. Typically, the perfect record for individual faces is conducted from the 3D face images, with a pose variety of ±45° rotation intensive and ±10° rotation in the image plane [44, 45]. In this way, a face image can therefore be captured from different surroundings (Figure 4).

In consideration of the security and secrecy needs, no wireless transmission network is allowed to build within the

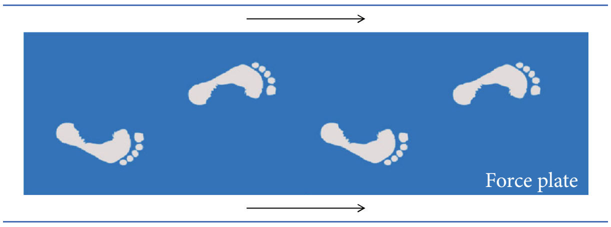

Figure 2: Force plate for GRF recording.

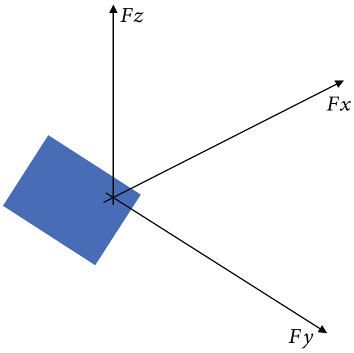

Figure 3: GRF component.

target area. As a result, the camera is connected to the signal processing module on the host computer with low-noise electric cable. In addition, the images of permitted individuals as well as the face recognition programs are collected beforehand and are stored as a dataset for real-time calling. When the face image of the coming person is detected, the data can be transferred from the camera to the host computer. The face recognition algorithms are run to process the image signals. We shall thus identify the person's identity by matching the faces from the database. Therefore, the users can further process the images via linking to the host computer.

4. Identity Verification Algorithm

The GRF signals and the facial images are collected through the aforementioned system while the person is stepping to the security area. In the interest of individual verification, we tend to fuse these data for processing and analysis. On this occasion, we shall thus define the primary procedures of data processing, which is exhibited in Figure 5.

4.1. GRF Testing Algorithm. During the gait analysis phase, the ground reaction forces are collected to be identified, whose schematic diagram of the system is presented in Figure 6. To start with, the GRF signals are conditioned into process able data for further investigation. The sliding window is employed for GRF data segmentation for continuous identification. Specifically, the data is filtered to remove the random noise from the sensor outputs. Furthermore, an extractor is used for gait feature extraction, from which the internal characteristics are derived from gait in time sequence. Mathematically, features characterize the data from every single analysis window without losing information. In this research, four different features are extracted to demonstrate the GRF variation, which are maximum value, average value, standard deviation, and kurtosis. Accordingly, the representation of individual gait is sent to the characteristic matcher to authenticate a walking person. The identification of GRF is conducted by using the SVM (support vector machine) classifier, which resolves problems of high-dimensional data as presented in [46]. The RBF (radial basis function) kernel is taken for data training and testing. At this stage, the gait pattern is compared with the template of one single person, which is picked from the database stored in the host computer. The force is first matched to a prespecific kind of GRF. Hereafter, the features are compared to the database of four feature parameters and their values. The identification process is exhibited in Algorithm 1 with θ as a preset threshold. As such, the gait representation is compared with that of all subjects within the storage. On this occasion, the output of the verification system can be either the identity of a previously enrolled individual or an alert message.

4.2. Face Recognition Algorithm. According to the aforementioned steps, a novel model is built up as shown in Figure 7. Originally, an $n \times m$ pixel image represents a face via the vector in an $n \times m$ dimensional space. Hence, the dimensionality reduction is a procedure of transforming a high-dimensional data set into a low-dimensional representation which retains most of the information [47]. In most cases, the dimensionality reduction is a preprocess of feature extraction. As for face recognition, we use the MPCA (multilinear principal component analysis) method for reducing the feature projection matrix of face images, which is a widely used multilinear algorithm that extracts features from multidimensional objects [48]. The outputs of the MPCA are sent to the feature extractor. In this paper, we take the LBP operator based on the exploration of [49]. Since the LBP operator has the window of 3×3, the gray value of the adjacent 8 pixels is compared with that of the center value. As long as the neighboring pixel value is greater than or equal to the center pixel value, the value of the target pixel is set as 1, otherwise set as 0. Consequently, the LBP eigenvalues of each pixel can be obtained to compose a feature spectrum. In order to get a real-time outcome, the similarity distance measure, which is a simple but effective recognition approach, is employed. Specifically, the L2 similarity distance measurement, whose purpose is to compute the L2 distance between the target face and those from the database, is taken to determine whether the two faces are the same or not. The creation of face dataset is applied to store the predefined individual facial images, which is the foundation of identity matching. Similar to the GRF analysis procedures, the face recognition algorithm is presented (Algorithm 2).

4.3. Decision-Making. Each of the subsystem provides a local result of the identification outcome. Compared to the identities from the database, the output value is normalized to be either 0 or 1 where 0 and 1 indicate the rejection and acceptance, respectively. The global decision, however, is computed by integrating the two outcomes. Commonly, the two outcomes are combined

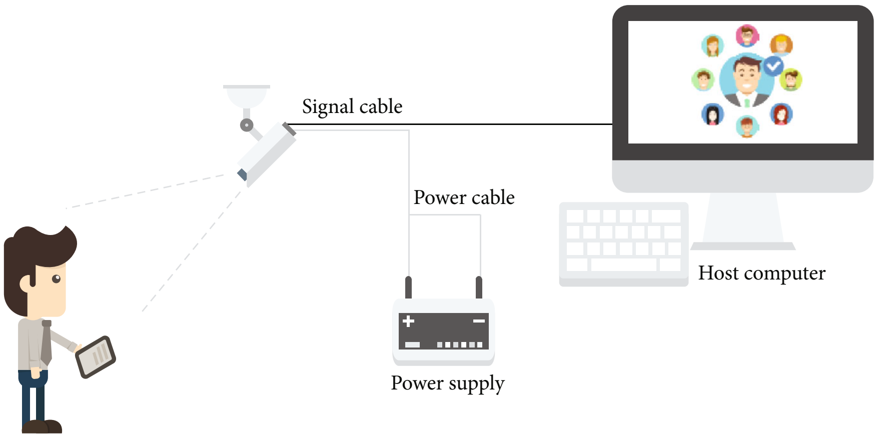

Figure 4: Face recognition system.

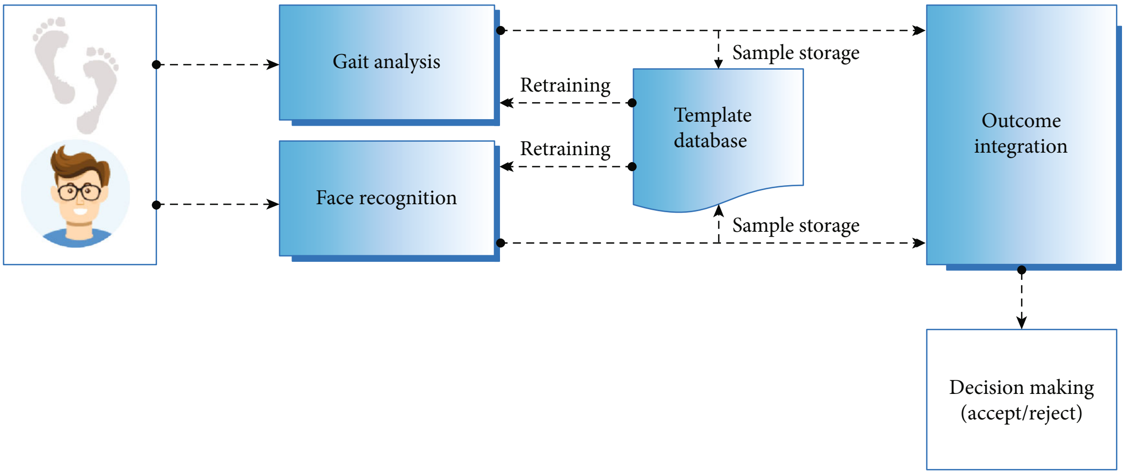

Figure 5: Identity verification based on integration of gait analysis and face recognition.

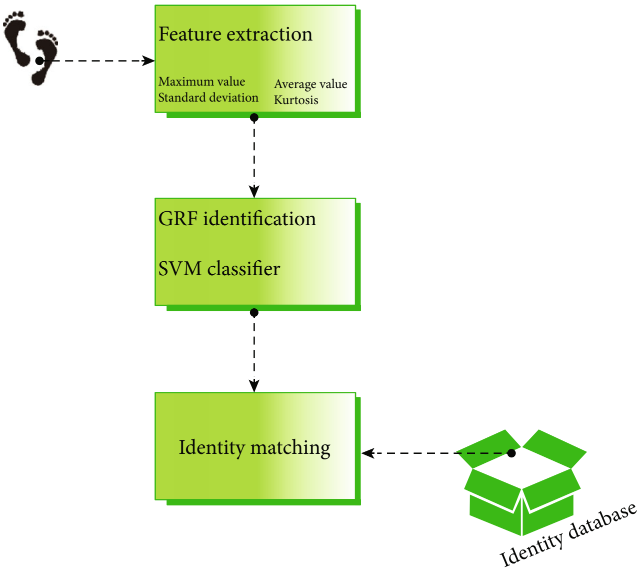

Figure 6: GRF processing flow.

by using the weighted average algorithm. In this way, the final decision is on the basic of the probability on the personal identity. As mentioned in Section 2, we employ the RAF for data integration in this paper. For every single feature, the fuzzy sets can be built up and we can therefore measure the significance of the rule. Further, a FAR base is established where all the frequent fuzzy item sets can be obtained.

The fuzzy decision is given based on the FAR. There is no need for the obtained signals entirely matching with the standard personal pattern. To estimate the individual identity, we employ the Gaussian curve membership function for data characterization. The membership within the fuzzy set is shown as follows:

$$\alpha = \exp\left[-\left(\frac{x-c}{\sigma}\right)^{2}\right], \qquad (6)$$

where c is the data center and σ is the variance. Moreover, the fuzzy matching for individual identity is presented as follows:

$$Fi\left(x_j\right) = \prod_{j=1}^{n} \alpha\left(x_j\right) = \prod_{j=1}^{n}\left[-\left(\frac{x-c_j}{\sigma}\right)^{2}\right]. \qquad (7)$$

```
Initialize feature extractor.
Initialize SVM based classifier.
while run do
Perform GRF detector to get gait set $\{X_i, Y_i, Z_i\}$.
Perform feature extractor to get gait feature set $\{X_i^F\}_1^n, \{Y_i^F\}_1^n, \{Z_i^F\}_1^n$
Perform classifier on detected gait feature set $\{D_j\}_1^k$ and get the probability $P(D_j)$.
if$P(D_j) \geq \theta$ then
    Accept $\{D_j\}_1^k$ as the target person, and its probability as $P(D_j)$.
else
    Output alarm information
end if
end while
```

Algorithm 1. GRF analysis.

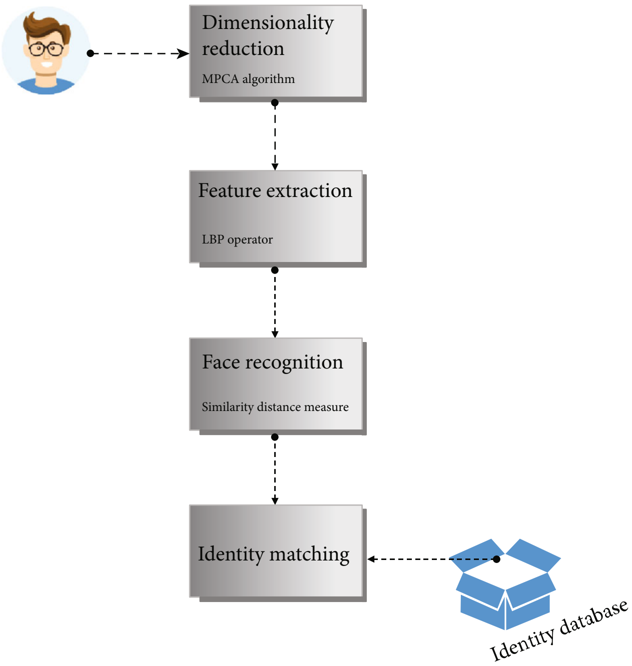

Figure 7: Face recognition flow.

The outcome of the maximum fuzzy matching degree can therefore be found. In terms of identity verification, the result corresponds to the fuzzy decision exactly, which is expressed as follows:

$$FI(x_j) = \max Fi(x_j). \quad (8)$$

5. Experiments

The evaluation of working performance of the propose method for individual verification is carried out. The equipment is deployed in front of a laboratory access of a college in the city of Shanghai. The current security area allows only 26 staff to get access. We collect the GRF signals of individuals from different types of shoes and facial images of different expressions and angles. In this way, 936 pieces of data are generated. The dataset is divided into three parts: 60% training data, 20% validation, and 20% testing data. The training procedure is performed on the training set, followed with the evaluation on the validation set. As long as expected results are obtained, the testing data is sent to the detector for individual identity verification. With the power supplied, GRF signals are recorded by the sensors on the force plate, while the face images are captured via the video camera. Both kinds of signals are transmitted to the computer through the electric cable in real time. The data processing procedure is implemented on the Dell server with two GTX-1080GPU, and the operating system is a 64-bit Ubuntu 16.4. One example of the waveforms of GRF signals and face images of one individual are presented in Figures 8 and 9. We verify the identity of these volunteers by the proposed method.

Initially, we train our method through the learning data in the dataset. The accuracy of identification shown in Equation (9) is determined by calculating the number of correctly recognized class instances (TP, true positives), the number of correctly recognized instances that do not belong to the class (TN, true negatives), and instances that either were incorrectly assigned to the class (FP, false positives) or were not recognized as class instances (FN, false negatives) [50]. The model is fine-tuned during the validation and evaluated during the testing.

$$\text{Accuracy} = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{TN} + \text{FP} + \text{FN}}. \quad (9)$$

Reported outcomes facilitate the evaluation of the proposed methods. At the first stage, the decisions based on gait analysis and face recognition are illustrated in Table 1. We can see that, for gait analysis outcome, all the errors are resulted from the rejected genuine users. In contrast, most errors of face recognition are caused by the accepted impostors.

The detection accuracy increases in line with the number of training samples (Figure 10). The proposed method is tested based on the inputs. In comparison, we initially present the outcomes by using only one kind of biometric

```
Initialize pre-processor.
Initialize feature extractor.
Initialize LBP operator.
while run do
Perform camera to get facial image $\{F_i\}_1^n$.
Perform pre-processor to reduce the high-dimensionality.
Perform feature extractor to get feature set $\{F_i^F\}_1^n$.
Perform LBP operator on image feature set $\{D_j\}_1^k$ and get the maximal confidence $conf(D_{\max})$.
if$conf(D_{\max}) \geq \theta$ then
  Accept $\{D_j\}_1^k$ as the target person, and its maximal confidence as $conf(D_{\max})$.
else
  Output alarm information
end if
end while
```

Algorithm 2. Face recognition.

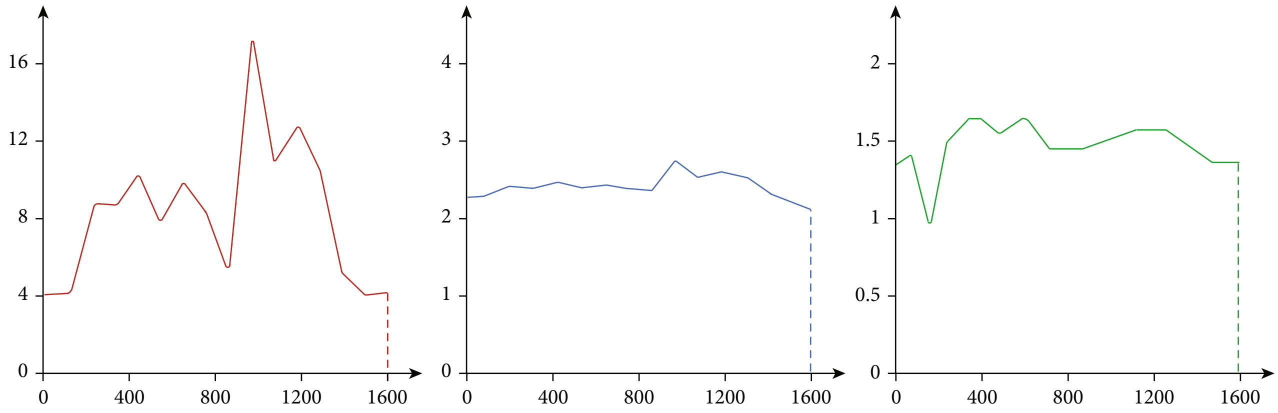

Figure 8: GRF outcomes of X, Y, and Z directions of the target person.

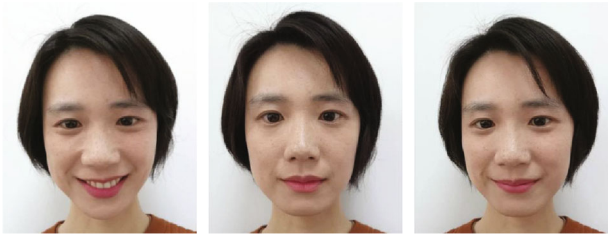

Figure 9: Face images of the target person.

Table 1: First stage outcomes.

Item	Rejected genuine users	Accepted impostors
Gait analysis	0.2	0.01
Face recognition	0.06	0.16

parameter detection. Moreover, the integration of data using weighted average based on the outcomes in Table 1 is given. The determination via FAR is applied to the two detection outcomes for decision-making. The detection errors of weighted average and FAR algorithm are given in Table 2 and Figure 11. By using the error analysis of Table 1, the weighted average algorithm has a quite even error on both rejected genuine users and accepted impostors. However, for the FAR determination, the errors caused by rejected genuine users are four times of those by accepted impostors. Experimental results on testing data are shown in Table 3.

6. Conclusion

In this paper, we mainly focus on a remote personal verification approach in the specific condition of security area monitoring. The integration of biometric parameters provides an opportunity to cater to the demands of noninvasion, high accuracy, and remote sensing based on the user's acceptability. This paper does present some contributions to the application of personal verification systems.

Firstly, the biometric parameters, i.e., GRF signals and facial images, are directly collected and transmitted for remote measurement with the devising and deployment of the detection system.

Secondly, both kinds of signals are processed by using the state-of-the-art algorithms. The signal detectors are

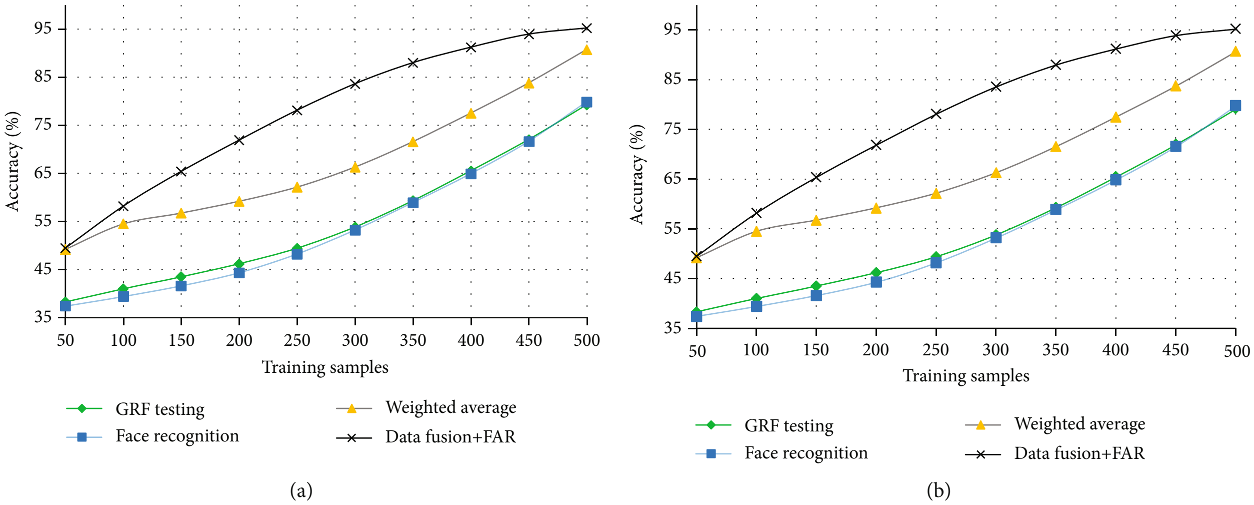

FIGURE 10: (a) Training accuracy of proposed methods. (b) Testing accuracy of proposed methods.

TABLE 2: Final outcomes.

Items	Rejected genuine users	Accepted impostors
Weighted average	0.04	0.05
FAR decision	0.04	0.01

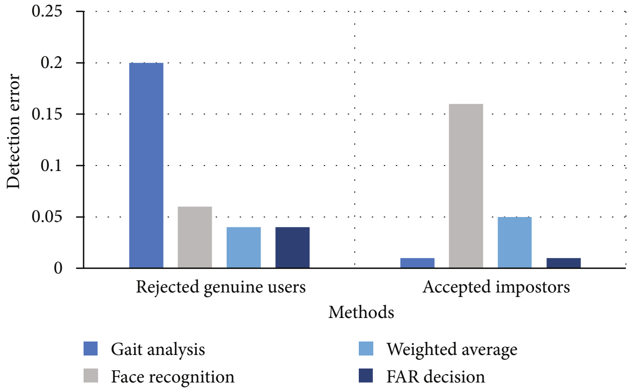

FIGURE 11: Detection error comparison.

TABLE 3: Working performance of different algorithms.

Methods	Training accuracy	Testing accuracy
Face recognition	83.1%	79.8%
GRF testing	86.9%	79.2%
Weighted average	92.3%	90.7%
FAR decision	97.3%	95.2%

established, and the signals are transmitted to identify the individual characteristics from a long distance.

Thirdly, the FAR algorithm is taken to better address the identification problem. An even higher detection accuracy is obtained because of the biometric signal integration.

Future steps will be taken to focus on the extension and validation of the current to more biometrics. In addition, the signal integration strategy will also be exploit, which aims to improve the personal verification accuracy.

Data Availability

The gait data and facial images used to support the findings of this study have not been made available because of the identity confidentiality of the users.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] A. Czyżewski, P. Hoffmann, P. Szczuko, A. Kurowski, M. Lech, and M. Szczodrak, “Analysis of results of large-scale multimodal biometric identity verification experiment,” *IET Biometrics*, vol. 8, no. 1, pp. 92–100, 2019.

[2] M. Gheisari, Q. Pham, M. Alazab, X. Zhang, C. Fernandez-Campusano, and G. Srivastava, “ECA: an edge computing architecture for privacy-preserving in IoT-based smart city,” *IEEE Access*, vol. 7, pp. 155779–155786, 2019.

[3] *Good practice guide, Identity proofing and verification of an individual*UK CEGC and Cabinet Office2018, https://webarchive.nationalarchives.gov.uk/20150514214143tf_/https://www.gov.uk/government/publications/identity-proofing-and-verification-of-an-individual.

[4] X. Wang, H. Xue, X. Liu, and Q. Pei, “A privacy-preserving edge computation-based face verification system for user authentication,” *IEEE Access*, vol. 7, pp. 14186–14197, 2019.

[5] L. Tseng, Y. Wu, H. Pan, M. Aloqaily, and A. Boukerche, “Reliable broadcast in networks with trusted nodes,” in *2019 IEEE Global Communications Conference (GLOBECOM)*, pp. 1–6, Waikoloa, HI, USA, December 2019.

[6] C.-T. Hsieh, C.-C. Han, C.-H. Lee, and K.-C. Fan, *Person authentication using nearest feature line embedding transformation and biased discriminant analysis*, International Carnahan Conference on Security Technology, Madrid, Spain, 2017.

[7] Y. Tian, Y. Li, X. Liu, R. H. Deng, and B. Sengupta, "PriBioAuth: privacy-preserving biometric-based remote user authentication," in *2018 IEEE Conference on Dependable and Secure Computing (DSC)*, pp. 1–8, Kaohsiung, Taiwan, 2018.

[8] A. L. M. Cuenca, Y. R. C. Dizon, H. A. Espinosa et al., "Development of plantar pressure in-sole system for diabetic peripheral neuropathy analysis using pressure mapping sensors," in *2019 IEEE 11th International Conference on Humanoid, Nanotechnology, Information Technology, Communication and Control, Environment, and Management (HNICEM)*, pp. 1–6, Laoag, Philippines, 2019.

[9] S. Hemalatha, "A systematic review on fingerprint based biometric authentication system," in *2020 International Conference on Emerging Trends in Information Technology and Engineering (ic-ETITE)*, pp. 1–4, Vellore, India, India, February 2020.

[10] R. A. Halim and A. W. R. Emanuel, "A review of iris recognition system ROI and accuracy," in *2020 International Conference on Smart Technology and Applications (ICoSTA)*, pp. 1–6, Surabaya, Indonesia, Indonesia, February 2020.

[11] A. Nilizadeh, W. Mazurczyk, C. Zou, and G. T. Leavens, "Information hiding in RGB images using an improved matrix pattern approach," in *2017 IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW)*, pp. 1407–1415, Honolulu, HI, 2017.

[12] J. Dąbroś, M. Iwaniec, M. Patyk, and J. Wesół, "Machine learning gait analysis algorithm for ontogenetic features compensation," in *2018 XIV-th International Conference on Perspective Technologies and Methods in MEMS Design (MEMSTECH)*, pp. 132–135, Zakarpattya, Ukraine, 2018.

[13] F. AL-Turjman and D. B. David, "Seamless authentication: for IoT-big data technologies in smart industrial application systems," in *IEEE Transactions on Industrial Informatics(Early Access)*, April 2020.

[14] D. A. Reynolds and R. C. Rose, "Robust text-independent speaker identification using Gaussian mixture speaker models," *IEEE Transaction on Speech and Audio Processing*, vol. 3, no. 1, pp. 72–83, 1995.

[15] M. Wang and Z. Yan, "Privacy-preserving authentication and key agreement protocols for D2D group communications," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 8, pp. 3637–3647, 2018.

[16] Y. Ma, L. Wu, X. Gu, J. He, and Z. Yang, "A secure face-verification scheme based on homomorphic encryption and deep neural networks," *IEEE Access*, vol. 5, pp. 16532–16538, 2017.

[17] M. P. Piromalis and G. Tsaramirsis, "A study of keeping low cost in sensors and μcontroller implementations for daily activities," in *2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom)*, pp. 1403–1407, New Delhi, 2016.

[18] J. S. Park, C. M. Lee, S. Koo, and C. H. Kim, "Gait phase detection using force sensing resistors," *IEEE Sensors Journal*, vol. 20, no. 12, pp. 6516–6523, 2020.

[19] B. J. Gow, J. M. Hausdorff, B. Manor et al., "Can tai chi training impact fractal stride time dynamics, an index of gait health, in older adults? Cross-sectional and randomized trial studies," *PLOS ONE*, vol. 12, no. 10, article e0186212, p. 17, 2017.

[20] A. H. Sodhro, L. Zongwei, S. Pirbhulal, A. K. Sangaiah, S. Lohano, and G. H. Sodhro, "Power-management strategies for medical information transmission in wireless body sensor networks," *IEEE Consumer Electronics Magazine*, vol. 9, no. 2, pp. 47–51, 2020.

[21] B. Roche, A.-L. Simon, S. Guilmin-Crépon et al., "Test-retest reliability of an instrumented electronic walkway system (GAITRite) for the measurement of spatio-temporal gait parameters in young patients with Friedreich's ataxia," *Gait and Posture*, vol. 66, pp. 45–50, 2018.

[22] S. Rogan, R. de Bie, and E. Douwe de Bruin, "Sensor-based foot-mounted wearable system and pressure sensitive gait analysis," *Zeitschrift für Gerontologie und Geriatrie*, vol. 50, no. 6, pp. 488–497, 2017.

[23] S. Pirbhulal, W. Wu, G. Li, and A. K. Sangaiah, "Medical information security for wearable body sensor networks in smart healthcare," *IEEE Consumer Electronics Magazine*, vol. 8, no. 5, pp. 37–41, 2019.

[24] J. Frank, "The production of visualization software to facilitate analysis of ground reaction force and vector data as applied to the study of human biomechanics," Department of Computer Science, The Cooper Union for the Advancement of Science and Art, New York City, New York, USA, 1999, Master Dissertation.

[25] F. Lin, A. Wang, Y. Zhuang, M. R. Tomita, and W. Xu, "Smart insole: a wearable sensor device for unobtrusive gait monitoring in daily life," *IEEE Transactions on Industrial Informatics*, vol. 12, no. 6, pp. 2281–2291, 2016.

[26] M. I. M. Refai, B.-J. F. van Beijnum, J. H. Buurke, and P. H. Veltink, "Portable gait lab: estimating 3D GRF using a pelvis IMU in a foot IMU defined frame," *IEEE Transactions on Neural Systems and Rehabilitation Engineering*, vol. 28, no. 6, pp. 1308–1316, 2020.

[27] C.-C. Wu, Y.-T. Wen, and Y.-J. Lee, "IMU sensors beneath walking surface for ground reaction force prediction in gait," *IEEE Sensors Journal*, vol. 20, p. 1, 2020.

[28] J. A. Antonino-Daviu, S. B. Lee, and E. G. Strangas, "Guest editorial special section on advanced signal and image processing techniques for electric machines and drives fault diagnosis and prognosis," *IEEE Transactions on Industrial Informatics*, vol. 13, no. 3, pp. 1257–1260, 2017.

[29] B. Lu, J.-C. Chen, C. D. Castillo, and R. Chellappa, "An experimental evaluation of covariates effects on unconstrained face verification," *IEEE Transactions on Biometrics, Behavior, and Identity Science*, vol. 1, no. 1, pp. 42–55, 2019.

[30] "Facial recognition system," https://http://en.m.wikipedia.org/wiki/Facial_recognition_system.

[31] D. S. S. Mahesh, T. M. Reddy, A. S. Yaswanth, C. Joshitha, and S. S. Reddy, "Facial detection and recognition system on Raspberry Pi with enhanced security," in *2020 International Conference on Emerging Trends in Information Technology and Engineering (ic-ETITE)*, pp. 1–5, Vellore, India, India, February 2020.

[32] D. B. M. Yin, A. A. Mukhlas, R. Z. W. Chik, A. T. Othman, and S. Omar, "A proposed approach for biometric-based authentication using of face and facial expression recognition," in *IEEE 3rd International Conference on Communication and Information Systems*, pp. 28–33, Singapore, Singapore, 2018.

[33] J. Dhamija, T. Choudhury, P. Kumar, and Y. S. Rathore, "An advancement towards efficient face recognition using live video feed," in *2017 International Conference on Computational Intelligence and Networks*, pp. 53–56, Odisha, India, October 2017.

[34] J. H. Liqiao and Q. I. Runhe, "Face recognition based on adaptive weighted HOG," *Computer Engineering and Applications*, vol. 53, no. 3, pp. 164–168, 2017.

[35] S. Haji and A. Varol, “Real time face recognition system,” in *4th International Symposium on Digital Forensics and Security*, pp. 107–111, Little Rock, AR, USA, 2016.

[36] Z. Li, L. Li, K. Yan, and C. Zhang, “Automatic image annotation using fuzzy association rules and decision tree,” *Multimedia Systems*, vol. 23, no. 6, pp. 679–690, 2017.

[37] S.-C. Cheng and Y.-P. Cheng, “An adaptive approach to quantify plant features by using association rule-based similarity,” *IEEE Access*, vol. 7, pp. 32197–32205, 2019.

[38] Y. Zhang, J. Qin, P. Shi, and Y. Kang, “High-order intuitionistic fuzzy cognitive map based on evidential reasoning theory,” *IEEE Transactions on Fuzzy Systems*, vol. 27, no. 1, pp. 16–30, 2019.

[39] S. Rathore, P. K. Sharma, A. K. Sangaiah, and J. J. Park, “A hesitant fuzzy based security approach for fog and mobile-edge computing,” *IEEE Access*, vol. 6, pp. 688–701, 2018.

[40] T. P. Trottier, *Design and evaluation of a force platform-type instrument to measure rate change in mass and centroid of an ablating body*, University of New Hampshire, Durham, USA, 2016, Master Dissertation, Department of Design,.

[41] *FD-11637 specifications*http://ni.com, http://www.ni.com/pdf/manuals/377309a.pdf.

[42] R. Kulandaivel, M. Balasubramaniam, F. Al-Turjman, L. Mostarda, M. Ramachandran, and R. Patan, “Intelligent data delivery approach for smart cities using road side units,” *IEEE Access*, vol. 7, pp. 139462–139474, 2019.

[43] F. Engmann, F. A. Katsriku, J.-D. Abdulai, K. S. Adu-Manu, and F. K. Banaseka, “Prolonging the lifetime of wireless sensor networks: a review of current techniques,” *Wireless Communications and Mobile Computing*, vol. 2018, 23 pages, 2018.

[44] S. Thakre, A. K. Gupta, and S. Sharma, “Secure reliable multimodel biometric fingerprint and face recognition,” in *2017 International Conference on Computer Communication and Informatics*, pp. 1–4, Coimbatore, India, January 2017.

[45] R. D. Labati, A. Genovese, E. Munoz, V. Piuri, and F. Scotti, “3-D granulometry using image processing,” *IEEE Transactions on Industrial Informatics*, vol. 15, no. 3, pp. 1251–1264, 2019.

[46] Z. Peng, C. Cao, Q. Liu, and W. Pan, “Human walking pattern recognition based on KPCA and SVM with ground reflex pressure signal,” vol. 2013, pp. 1–12, 2013.

[47] Y. Li, X. Chen, Y. Lin, G. Srivastava, and S. Liu, “Wireless transmitter identification based on device imperfections,” *IEEE Access*, vol. 8, pp. 59305–59314, 2020.

[48] Y. Fu, Y. Liu, and Z. Gao, “Multiple actuator fault classification in wind turbine systems using multi-linear principal component analysis techniques,” in *2019 25th International Conference on Automation and Computing (ICAC)*, pp. 1–6, Lancaster, United Kingdom, 2019.

[49] X. M. Zhao and C. B. Wei, “A real-time face recognition system based on the improved LBPH algorithm,” in *2017 IEEE 2nd International Conference on Signal and Image Processing*, pp. 72–76, Singapore, Singapore, August 2017.

[50] C.-L. Liu, W.-H. Hsaio, C.-H. Lee, T.-H. Chang, and T.-H. Kuo, “Semi-supervised text classification with universum learning,” *IEEE Transactions on Cybernetics*, vol. 46, no. 2, pp. 462–473, 2016.